Red Hat Certificate System 7.3

Release Notes

Updates for RHSA-2010:0602

Copyright © 2009 Red Hat, Inc.
Copyright © 2009 Red Hat, Inc..

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at *http://creativecommons.org/licenses/by-sa/3.0/*. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, MetaMatrix, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

Java® is a registered trademark of Oracle and/or its affiliates.

XFS® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

All other trademarks are the property of their respective owners.

1801 Varsity Drive
Raleigh, NC 27606-2072 USA
Phone: +1 919 754 3700
Phone: 888 733 4281
Fax: +1 919 754 3701

August 6, 2010 (update)

1. New Features in Red Hat Certificate System 7.3 2
    1.1. Registration Authority 2
    1.2. SCEP 3
    1.3. Auto-enrollment Proxy 3
2. Platform Support 4

2.1. Server Support 4
2.2. Client Support 5
2.3. Other Required Software 5
2.4. Optional Server Hardware 6
2.5. Optional Client Hardware 6
3. Installation and Deployment Notes 6
3.1. Obtaining Packages 6
3.2. Installation Notes 7
3.3. Required JRE and JDK 7
3.4. TPS Subsystem Considerations 10
3.5. Directory Server Information 10
3.6. Source RPMs 10
4. Known Issues 11
4.1. Reconfiguring the Red Hat Certificate System Subsystems to Prevent a Potential TLS-Related Man-in-the-Middle Attack 11
4.2. Manually Adding a New Port to the RA 15
4.3. Viewing Enterprise Security Client Diagnostics Logs 17
4.4. Other Known Issues 17
5. Documentation 19
6. Copyright and Third-Party Acknowledgments 20
7. Document History 24

These release notes contain important information available at the time of release for Red Hat Certificate System 7.3. New features, system requirements, installation notes, known problems, resources, and other current issues are addressed here. Read this document before beginning to use Red Hat Certificate System.

1. New Features in Red Hat Certificate System 7.3

1.1. Registration Authority

Red Hat Certificate System 7.3 supports a stand-alone Registration Authority (RA), which supports the automatic issue of certificates to devices and servers.

The RA subsystem is a front-end subsystem to the Certificate Authority (CA), and it performs local authentication, requestor information gathering and request validation. It is responsibile for fowarding requests to the CA for signing.

The RA can be configured to authenticate incoming requests, or to route the request to appropriate personnel for approval before forwarding the request to the CA for certificate creation. The RA is typically set up outside of the firewall, while the CA is behind the firewall.

1.1.1. Enrollment Types

The RA currently provides the following enrollment types:

- SCEP enrollment
- Server certificate enrollment
- User certificate enrollment and renewal

- RA Agent enrollment

The RA also supports:

- Status checks of Certificate Requests
- Certificate retrieval
- Email notification on Certificate Request creation and approval

1.1.2. RA Roles

The RA supports the following roles:

- End Users - people who submit enrollment requests
- RA Agents - privileged RA users who are responsible for daily operation such as request approval
- Administrators - people responsible for installing and configuring the RA. Administrators can also create new users and assign them as Agents.

1.2. SCEP

SCEP (Simple Certificate Enrollment Protocol) is a protocol designed by Cisco. It specifies a way for a router to communicate with RAs and CAs for enrollment. Red Hat Certificate System 7.3 enables routers to enroll for a certificate from an RA using this protocol.

Routers can communicate with the RA using the SCEP protocol to:

- Retrieve CA certificates
- Submit a Certificate Request
- Retrieve the issued certificate
- Submit a status request if the Certificate Request is pending

SCEP specifies two modes of operation:

- RA mode
- CA mode

In RA mode, the enrollment request is encrypted with the RA signing certificate. In CA mode, the request is encrypted with the CA signing certificate. The current Certificate System RA adn CA subsystems are implement so that SCEP is only supported in CA mode.

1.3. Auto-enrollment Proxy

Red Hat Certificate System 7.3 supports an auto-enrollment proxy (AEP) for Windows®, which allows users and computers in a Microsoft Windows® domain to automatically enroll for certificates issued from Certificate System.

Designed to integrate seamlessly with an existing Windows® infrastructure, the AEP module minimizes administration overhead:

- Users and computers registered in a Windows® domain can automatically discover the location of the proxy on their network
- Computers in a domain can automatically compose a certificate request, and submit it to a Red Hat Certificate System CA via the proxy
- The Kerberos authentication mechanism built into Windows® authenticates these certificate requests
- When the CA issues a certificate, it is automatically installed into the requesting application

AEP can issue certificates for domain controllers (including backup controllers), web servers, computers, and users.

For more information about this feature, see *http://directory.fedoraproject.org/wiki/Auto_Enroll_Documentation*.

2. Platform Support

This section contains information related to installing Red Hat Certificate System 7.3, including hardware and platform requirements and prerequisites.

2.1. Server Support

The Certificate System subsystems are supported on the following platforms:

- Red Hat Enterprise Linux AS and ES 4 for i386 AMD and Intel
- Red Hat Enterprise Linux AS and ES 4 for AMD64 and Intel EM64T
- Sun Solaris 9 for SPARC 64-bit

2.1.1. Server Requirements

Component	Details
CPU	Intel — 2.0 GHz Pentium 4 or faster
RAM	1 GB (required)

Hard disk storage space	Total is approximately 5 GB
	• Total transient space required during installation: 1 GB
	• Hard disk storage space required for installation:
	  • Space required to set up, configure, and run the server: approximately 2 GB
	  • Additional space for database growth in pilot deployment: approximately 1 GB
	  • Total disk storage space for installation: approximately 1 GB

Table 1. Red Hat Enterprise Linux Server Requirements

2.1.2. Red Hat Enterprise Linux Considerations

Before installing the Certificate System packages, ensure that the proper dependencies are installed on the Red Hat Enterprise Linux system.

The following package groups and packages must be installed on all Red Hat Enterprise Linux systems:

- dialup (package group)
- gnome-desktop (package group)
- compat-arch-support (package group)
- web-server (package group)
- kernel-smp (package)
- e2fsprogs (package)
- firefox (package)

On 64-bit Red Hat Enterprise Linux platforms, ensure that the 64-bit (x86_64) **compat-libstdc++** libraries are installed, and not only the 32-bit (i386) libraries. To confirm this, run the following command as `root`:

```
rpm -qa --queryformat 'compat-libstdc++-%{VERSION}-%{RELEASE}.%{ARCH}.rpm | grep x86_64
```

Numerous libraries should be displayed.

2.2. Client Support

The Enterprise Security Client is supported on the following platforms:

- Apple Macintosh OS X 10.4.x (Tiger on Power PC and Intel)
- Microsoft Windows XP Professional (i386)
- Red Hat Enterprise Linux AS 4 (i386)
- Red Hat Enterprise Linux ES 4 (i386)
- Red Hat Enterprise Linux AS 4 for AMD64 and Intel EM64T
- Red Hat Enterprise Linux ES 4 for AMD64 and Intel EM64T

2.3. Other Required Software

- *Red Hat Directory Server 7.1 or 8.x.*

  The source code and binaries for this component are available at *https://rhn.redhat.com*, through the Red Hat Directory Server channels.

IMPORTANT

With the updates from Errata RHSA-2010:0602, there is a conflict between the **`fortitude-mod_nss`** package installed with Red Hat Directory Server 8.x and the packages installed for the RA and TPS. A Directory Server version 8.x instance cannot be installed on the same machine as either the RA or TPS subsystem, then.

On Red Hat Enterprise Linux, the conflicting package is **`fortitude-mod_nss-1.0.8-3.el4idm`**. On Solaris, the conflicting package is **`fortitude-mod-nss-1.0.8-1.sol9idm`**.

- *A web browser that supports SSL.*

  It is strongly recommended that users such as agents or administrators use Mozilla Firefox. End-entities should use Mozilla Firefox or Microsoft Internet Explorer.

  The only browser that is fully-supported for the HTML-based instance configuration wizard is Mozilla Firefox.

2.4. Optional Server Hardware

Red Hat Certificate System supports Chrysalis-ITS LunaSA Hardware Security Module (HSM).

Architecture	Version
Firmware	4.5.2
Appliance Software	3.2.4
Client Software	3.2.4

2.5. Optional Client Hardware

- Axalto Global Platform compatible Cyberflex eGate token

3. Installation and Deployment Notes

The following sections contain important installation, configuration, and deployment information for Red Hat Certificate System 7.3.

3.1. Obtaining Packages

Red Hat Network (*http://rhn.redhat.com*) is the software distribution mechanism for most Red Hat customers. Account login information for Red Hat Network, including entitlements for the Red Hat Certificate System 7.3 release, is required to download this software from Red Hat Network. After logging into Red Hat Network, go to the appropriate Red Hat Certificate System 7.3 channel to download the packages for the selected Red Hat Enterprise Linux platform.

NOTE

The source code for Red Hat Directory Server 7.1 is included with the ISO image downloaded for the 32-bit Red Hat Enterprise Linux version. Red Hat Certificate System itself is not yet open source.

Red Hat Enterprise Linux systems can upgrade or download Red Hat Certificate System using **`up2date`**.

3.2. Installation Notes

- Packages are non-relocatable. The Red Hat Certificate System base packages can not be installed to a user-designated location.
- Do not use the autorun feature of the CD drive. If you use the autorun feature with a CD created from the ISO image, all subsystems (CA, DRM, OCSP, TKS, and TPS) as well as the Enterprise Security Client are installed on the system by default.

  The preferred alternative is to run the installation scripts provided for the server, or to follow the installation instructions in the *Red Hat Certificate System 7.3 Administration Guide*.
- Ensure that you remove any existing installations of **`*sqlite*`** RPM files for the RA, specifically **`libsqlite`**. The **`sqlite-`***XX* RPM files that ship with RA will cause conflicts with those files.

3.3. Required JRE and JDK

IMPORTANT

To address security issues in both IBM and Solaris JDK and JRE, certain updates are required for both Red Hat Enterprise Linux and Solaris systems. Certificate System is not directly affected by the security issues in the JDK and JRE packages, but, as a precautionary measure, make sure that the appropriate versions of these packages are installed.

3.3.1. Required JRE and JDK for Red Hat Enterprise Linux 4

Red Hat Enterprise Linux 4 versions of Red Hat Certificate System require Java 1.5.0 Java Runtime Environment (JRE). Certificate System does not support other versions of the JRE. This JRE is required for running Tomcat, among other applications for the Certificate System.

Likewise, the IBM JDK must be present on Red Hat Enterprise Linux systems. See *http://kbase.redhat.com/faq/FAQ_54_4667.shtm* for more information.

These packages are recommended for 32-bit Red Hat Enterprise Linux systems:

- java-1.5.0-ibm-1.5.0.11.1-1jpp.3.el4.i386.rpm (JRE)
- java-1.5.0-ibm-devel-1.5.0.11.1-1jpp.3.el4.i386.rpm (JDK)

These packages are recommended for 64-bit Red Hat Enterprise Linux systems:

- java-1.5.0-ibm-1.5.0.11.1-1jpp.3.el4:1.x86_64.rpm (JRE)
- java-1.5.0-ibm-devel-1.5.0.11.1-1jpp.3.el4:1.x86_64.rpm (JDK)

WARNING

Both the 32-bit xSeries (Intel-compatible) and 64-bit AMD/Opteron/EM64T versions of the IBM J2SE JRE 5.0 RPM packages available through the IBM download site are packaged in a format which is incompatible with Certificate System 7.3.

Both 32-bit and 64-bit Red Hat Enterprise Linux 4 packages are available. Make sure to install the appropriate version for your system.

- *Section 3.3.1.1, "Security Fixes in the Required Red Hat Enterprise Linux 4 JRE and JDK Packages"*
- *Section 3.3.1.2, "Installing the Required JRE and JDK on Red Hat Enterprise Linux 4"*

3.3.1.1. Security Fixes in the Required Red Hat Enterprise Linux 4 JRE and JDK Packages

Certain security issues for the IBM JRE and JDK were released in two erratas. These changes are listed in *Table 2, "CVEs Fixed in JRE/JDK Errata Updates"*. Although none of these problems directly affect Red Hat Certificate System 7.3, the latest errata should be applied as a security precaution.

Bug	Description
Errata RHSA-2007-0829[1]	
Bug #239660	CVE-2007-2435 javaws vulnerabilities
Bug #250725	CVE-2007-2788 Integer overflow in the embedded ICC profile image parser in Sun Java Development Kit
Bug #250729	CVE-2007-2789 BMP image parser vulnerability
Bug #242595	CVE-2007-3004 Integer overflow in IBM JDK's ICC profile parser
Bug #250733	CVE-2007-3005 Unspecified vulnerability in Sun JRE
Bug #246765	CVE-2007-3503 HTML files generated with Javadoc are vulnerable to a XSS
Bug #248864	CVE-2007-3655 A buffer overflow vulnerability in Java Web Start URL parsing code
Bug #249533	CVE-2007-3922 Vulnerability in the Java Runtime Environment May Allow an Untrusted Applet to Circumvent Network Access Restrictions
Errata RHSA-2010-0130[2]	
Bug #533125	CVE-2009-3555 TLS: MITM attacks via session renegotiation

Table 2. CVEs Fixed in JRE/JDK Errata Updates

3.3.1.2. Installing the Required JRE and JDK on Red Hat Enterprise Linux 4

1. Download the **java-1.5.0-ibm-1.5.0.11.1-1jpp.3.el4** and **java-1.5.0-ibm-devel-1.5.0.11.1-1jpp.3.el4** packages from the latest errata update, *Errata RHSA-2010-0130*[3].

2. Install the packages. For example, for the 32-bit packages:

```
rpm -Uvh java-1.5.0-ibm-1.5.0.11.1-1jpp.3.el4.i386.rpm java-1.5.0-ibm-
devel-1.5.0.11.1-1jpp.3.el4.i386.rpm
```

3. Make sure that the IBM Java 1.5.0 is selected as the default JRE and the the IBM 5.0 JDK is available:

```
/usr/sbin/alternatives --config java

There are 2 programs which provide 'java'.

  Selection    Command
-----------------------------------------------
*+ 1           /usr/lib/jvm/jre-1.5.0-ibm/bin/java
   2           /usr/lib/jvm/jre-1.4.2-sun/bin/java

Enter to keep the current selection[+], or type selection number: 1

/usr/sbin/alternatives --config javac

There are 2 programs which provide 'javac'.

  Selection    Command
-----------------------------------------------
   1           /usr/lib/jvm/java-1.5.0-bea/bin/javac
*+ 2           /usr/lib/jvm/java-1.5.0-ibm/bin/javac
```

3.3.2. Required JRE and JDK for Sun Solaris

The recommended version is Sun JDK and JRE 5.0 Update 24. This is available from *http://java.com/en/download/manual.jsp#sol*.

Red Hat Certificate System 7.3 uses the native JRE and JDK packages on Solaris to operate. Certain security issues for the Sun JRE and JDK have been addressed in several recent erratas. These changes are listed in *Table 3, "CVEs Fixed in JRE/JDK Errata Updates"*. Although none of these problems directly affect Red Hat Certificate System 7.3, the latest errata should be applied as a security precaution.

Other vulnerabilities to the Sun JDK and JRE are summarized at *"Advance notification of Security Updates for Java SE"*[4] page from Sun Microsystems.

Bug	Description
Errata RHSA-2007-0963[5]	
Bug #321951	CVE-2007-5232 Security Vulnerability in Java Runtime Environment With Applet Caching

[4] http://blogs.sun.com/security/entry/advance_notification_of_security_updates7

Bug	Description
Bug #321961	CVE-2007-5238 Vulnerabilities in Java Web Start allow to determine the location of the Java Web Start cache
Bug #321981	CVE-2007-5239 Untrusted Application or Applet May Move or Copy Arbitrary Files
Bug #321991	CVE-2007-5240 Applets or Applications are allowed to display an oversized window
Bug #324351	CVE-2007-5273 Anti-DNS Pinning and Java Applets with HTTP proxy
Bug #324361	CVE-2007-5274 Anti-DNS Pinning and Java Applets with Opera and Firefox

Table 3. CVEs Fixed in JRE/JDK Errata Updates

3.4. TPS Subsystem Considerations

- TPS subsystems installed on a Red Hat Enterprise Linux system require a local installation of the Apache 2.0.x web server.
- The TPS subsystem cannot be cloned.
- The TPS subsystem cannot be installed on the same machine as Red Hat Directory Server 8.x instances because of a conflict with the mod_nss packages.

3.5. Directory Server Information

All subsystems require access to Red Hat Directory Server 7.1 or 8.x on either the local machine (if it is also a 32-bit Red Hat Enterprise Linux platform) or a remote machine (acceptable platforms are 32-bit Red Hat Enterprise Linux 4, 32-bit Solaris 9 for SPARC, or 64-bit Solaris 9 for SPARC).

IMPORTANT

With the updates from Errata RHSA-2010:0602, there is a conflict between the **`fortitude-mod_nss`** package installed with Red Hat Directory Server 8.x and the packages installed for the RA and TPS. A Directory Server version 8.x instance cannot be installed on the same machine as either the RA or TPS subsystem, then.

On Red Hat Enterprise Linux, the conflicting package is **`fortitude-mod_nss-1.0.8-3.el4idm`**. On Solaris, the conflicting package is **`fortitude-mod-nss-1.0.8-1.sol9idm`**.

3.6. Source RPMs

Red Hat Certificate System 7.3 is not an open-source product. Consequently, source RPMs are only available for third-party packages.

NOTE

Several of these third-party packages may issue warnings when they are installed because they may contain the UID and GID of their original packager.

4. Known Issues

4.1. Reconfiguring the Red Hat Certificate System Subsystems to Prevent a Potential TLS-Related Man-in-the-Middle Attack

Transport Layer Security (TLS) is a protocol which establishes a secure connection between a client and a server. Marsh Ray of PhoneFactor discovered a flaw in the TLS protocol itself which could allow an attack to insert plain text into an existing session during a TLS renegotiation operation.

The Educated Guesswork blog has a good description of this kind of attack at *http://www.educatedguesswork.org/2009/11/understanding_the_tls_renegoti.html*.

Either a client or a server may request a renegotiation of an existing TLS/SSL session (for instance, to renew session encryption keys or to use different cipher suite). When TLS/SSL is used to secure access to an HTTP service and a client attempts to access some protected resource, server-initiated renegotiation asks client to authenticate with a certificate.

However, the TLS/SSL protocols did not use any mechanism to verify that session peers do not change during the session renegotiation. Therefore, a man-in-the-middle attacker could use this flaw to open TLS/SSL connections to the server, send attacker-chosen request to the server, trigger the renegotiation (either by directly requesting it or by attempting to access protected resource, resulting in server-initiated renegotiation) and splice victim's initial connection attempt to an existing TLS/SSL session. Depending on the application-layer protocol, this may lead to attacker request being performed by the server as if authenticated using victim's credentials or using data from victim's request. After the renegotiation, attacker can no longer decrypt communication between the client and the victim, so this attack is also referred to as a "blind prefix injection" attack. Eric Rescorla's blog post "Understanding the TLS Renegotiation Attack" provides additional details about this flaw.

In Certificate System, this kind of session renegotiation occurs if a user connects to an end-entity port that doesn't require client authentication, but then attempts to submit a certificate enrollment form for an enrollment profile that requires client authentication. The Certificate System server requests and then parses a client certificate for the user.

For both client-initiated and server-initiated renegotiation to be fixed, then both the client and server need to be updated to apply the resolution in RFC 5746. For Certificate System subsystems, this means applyng *Errata RHBA-2010:0170*[6] and *Errata RHBA-2010:0165*[7], plus these configuration changes, which resolve the man-in-the-middle vulnerability. Certificate System supports several different clients:

- Certificate System and third-party RA subsystems (used by both regular users and SCEP services)
- TPS subsystems, which connect to the CA for token operations
- The Windows Autoenrollment Proxy

[6] https://rhn.redhat.com/errata/RHBA-2010-0170.html
[7] https://rhn.redhat.com/errata/RHBA-2010-0165.html

- Web browsers, which are used by users to connect to the CA's end-entities pages

Updating the system NSS packages on any system that hosts a Certificate System subsystem will take care of all subsystem communication. When the NSS packages are updated, the CA-RA and CA-TPS connections will use the new session renegotiation protocol and all of the operations will proceed as normal.

Additional configuration changes may need to be made for the Windows auto-enrollment proxy or third-party RAs if those systems aren't updated to use the new renegotiation protocol. Contact Red Hat support for information on what needs to be done for those clients.

It is unclear on when browser clients will have updates available and applied to use the new session renegotiation protocol. If these clients aren't updated, but the server is, then the connections to the subsystem server may fail.

NOTE

These changes are not required if all clients accessing Certificate Systems are upgraded to support RFC 5746.

IMPORTANT

In Certificate System 7.3, no port is configured to require client authentication at the initial connection. The workaround in these release notes configures the agent secure port to require client authentication and directs requests for profiles that require client authentication to this port.

The workarounds here assume that Certificate System has been configured to use separate agent, end-entities, and admin ports. However, port separation is only available on Certificate System 7.3 if the server is updated to the latest version and then the subsystems are manually configured to use port separation.

Procedure 1. For the CA

1. Update the NSS packages by installing the system **`nss`** packages.

```
up2date nss
```

2. Before making any edits to the CA configuration, back up the following files:
   - /var/lib/*instance_name*/conf/server.xml
   - /var/lib/*instance_name*/web-apps.ee/ca/ee/ca/ProfileSelect.template
3. Open the **`server.xml`** file.

```
vim /var/lib/instance_name/conf/server.xml
```

4. In the **`server.xml`** file, change the **`clientAuth`** directive in the agent connector to **`true`**.

```
<Connector name="Agent" port="9443" maxHttpHeaderSize="8192"
```

```
        maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
        enableLookups="false" disableUploadTimeout="true"
        acceptCount="100" scheme="https" secure="true"
        clientAuth="true" sslProtocol="SSL"
```

5. Open the profile selection template.

```
vim /var/lib/instance_name/web-apps.ee/ca/ee/ca/ProfileSelect.template
```

6. Replace value in the **uri** line with the URL to the agent port. The original line is:

```
uri = 'profileSubmitSSLClient';
```

The updated line will look like the following:

```
uri = 'https://server.example.com:9444/ca/ee/ca/profileSubmitSSLClient';
```

7. Create a new end-entities web services directory to contain the files for the new URL referenced in the **ProfileSelect.template** file.

```
mkdir -p /var/lib/instance_name/webapps/ca/ee/ca

cp /var/lib/instance_name/webapps.ee/ca/ee/ca/ProfileSubmit.template /var/
lib/instance_name/webapps/ca/ee/ca

cp /var/lib/instance_name/webapps.ee/ca/ee/ca/ProfileSubmit.html /var/lib/instance_name/
webapps/ca/ee/ca/ProfileSubmit.html

chown -R pkiuser: /var/lib/instance_name/webapps/ca/ee
```

8. Restart the CA. For example:

```
/etc/init.d/rhpki-ca restart
```

Procedure 2. For the DRM

1. Update the NSS packages by installing the system **nss** packages.

```
up2date nss
```

2. First, in the CA, edit the **CS.cfg** file to contain the connector information with the agent's SSL port. For example:

```
vim /var/lib/rhpki-ca/conf/CS.cfg

ca.connector.KRA.port=10443
```

3. Then, for the DRM, open the **server.xml** file.

```
vim /var/lib/rhpki-kra/conf/server.xml
```

4. Change the **clientAuth** directive in the agent connector to true. For example:

```
<Connector name="Agent" port="10443" maxHttpHeaderSize="8192"
        maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
        enableLookups="false" disableUploadTimeout="true"
        acceptCount="100" scheme="https" secure="true"
        clientAuth="true" sslProtocol="SSL"
```

5. Restart the subsystem. For example:

```
/etc/init.d/rhpki-kra restart
```

Procedure 3. For the OCSP and TKS

1. Update the NSS packages by installing the system **`nss`** packages.

```
up2date nss
```

2. Open the **`server.xml`** file.

```
vim /var/lib/instance_name/conf/server.xml
```

3. Change the **`clientAuth`** directive in the agent connector to **`true`**. For example:

```
<Connector name="Agent" port="11443" maxHttpHeaderSize="8192"
        maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
        enableLookups="false" disableUploadTimeout="true"
        acceptCount="100" scheme="https" secure="true"
        clientAuth="true" sslProtocol="SSL"
```

4. Restart the subsystem. For example:

```
/etc/init.d/rhpki-ocsp restart
```

Procedure 4. For the TPS

1. Update the NSS packages by installing the system **`nss`** packages and install the new TPS packages.

```
up2date nss pki-tps
```

2. *On Linux systems only.* For an existing subsystem, edit the init script to preload the system NSS library rather than **`dirsec-nss`**.

```
vim /etc/init.d/instance_name
```

3. Remove the line:

```
LD_PRELOAD="/usr/lib64/dirsec/libssl3.so ${LD_PRELOAD}"
```

   Replace it with the following:

```
LD_PRELOAD="/usr/lib64/libssl3.so ${LD_PRELOAD}"
```

On 32-bit systems, the path is **/usr/lib/**.

4. Restart the subsystem. For example:

```
/etc/init.d/rhpki-tps restart
```

Procedure 5. For the RA

1. Update the NSS packages by installing the system **nss** packages and install the new RA packages.

```
up2date nss pki-ra
```

2. *On Linux systems only.* For an existing subsystem, edit the init script to preload the system NSS library rather than **dirsec-nss**.

```
vim /etc/init.d/instance_name
```

3. Remove the line:

```
LD_PRELOAD="/usr/lib64/dirsec/libssl3.so ${LD_PRELOAD}"
```

Replace it with the following:

```
LD_PRELOAD="/usr/lib64/libssl3.so ${LD_PRELOAD}"
```

On 32-bit systems, the path is **/usr/lib/**.

4. Restart the subsystem. For example:

```
/etc/init.d/rhpki-ra restart
```

4.2. Manually Adding a New Port to the RA

An SSL port must be added to the RA's **nss.conf** file to allow client authentication. This is is described in *Bug 229246*[8].

The default RA server has an optional port for performing SSL client authentication. It is expected that the agent and administration users will select the appropriate certificate to perform SSL authentication when asked, while users will just cancel out of the certificate selection process, if asked. The problem with this approach is that if an user cancels out of the certificate selection process, and chooses to renew a certificate (*Bug 233274*[9]), then the certificate selection process is automatically skipped, thus causing an error during certificate renewal.

[8] https://bugzilla.redhat.com/show_bug.cgi?id=229246
[9] https://bugzilla.redhat.com/show_bug.cgi?id=233274

This forces an user who wishes to renew a certificate to select the certificate to be renewed the first time they are asked to authenticate. This is awkward. To avoid this, provide a second port to handle only end-entity operations.

1. Open the configuration directory:

```
cd /var/lib/rhpki-ra/conf
```

2. Edit the **nss.conf** file:

   a. At the top, add another **Listen** line with a different port. For example:

```
Listen 0.0.0.0:12889
```

   b. Search for an existing **<VirtualHost ...> </VirtualHost>** container, copy the entire container and paste it at the end. Change the new container's port number to the new port. For example:

```
<VirtualHost _default_:12891>
```

   c. Go to the original **<VirtualHost ...>** entry, and change the value of **NSSVerifyClient** from **optional** to **require**.

   d. Go to the new **<VirtualHost ...>** entry, and change the value of **NSSVerifyClient** from **optional** to **none**.

   e. Save and exit.

3. Edit the **CS.cfg** file:

   a. Search for **service.securePort** and add the following line below it:

```
service.secureEePort=12891
```

   b. Save and exit.

4. Open the document root directory:

```
cd /var/lib/rhpki-ra/docroot
```

   a. Edit the **index.cgi** file. Search for **securePort**, and make a similar line with **secureEePort**. For example:

```
$::symbol{secureEePort} = $cfg->get("service.secureEePort");
```

   b. Edit the **index.vm** file. Search for **SSL End Users** and change the **href** line to use the new secure end-entities port (**secureEePort**). For example:

```
<a href="https://$machineName:$secureEePort/ee/index.cgi">SSL End Users Services</a>
```

   c. Save both files and exit.

5. Restart the RA system.

4.3. Viewing Enterprise Security Client Diagnostics Logs

The Enterprise Security Client events are not visible in the diagnostics logs, as noted in *Bug 234887*[10]. It is possible to configure the logs manually so tha they can be viewed in the diagnostics window or with a text editor.

On Mac:

1. Go to **`/Applications/ESC.app/Contents/MacOS`**.
2. Create an **`esc.sh`** file, as follows:

```
#!/bin/sh
NSPR_LOG_FILE=~/Library/"Application Support"/ESC/Profiles/esc.log
NSPR_LOG_MODULES=tray:2,coolKeyLib:2,coolKey:2,coolKeyNSS:2,coolKeySmart:2,coolKeyHandler:2
BASE_DIR=`dirname $0`
$BASE_DIR/xulrunner &
```

3. Go to **`/Applications/ESC.app/Contents/MacOS`**.
4. Run **`./esc.sh`**.
5. View the logs in the Enterprise Security Client or in the user's profile directory.

On Windows:

1. Open the **`C:\Program Files\RedHat\ESC`** directory.
2. Create an **`esc.bat`** file, as follows:

```
@echo off
SET NSPR_LOG_MODULES-
tray:2,coolKeyLib:2,coolKey:2,coolKeyNSS:2,coolKeySmart:2,coolKeyHandler:2
set NSPR_LOG_FILE=%USERPROFILE%\Application Data\RedHat\ESC\esc.log esc.exe
```

4.4. Other Known Issues

These are other known issues in Red Hat Certificate System 7.3, with workarounds when appropriate.

Bug Number	Description	Workaround
224612	During installation, there are RA SQLite dependency errors on 64-bit systems. This bug is caused by a configuration issue on the machine that the 64-bit RA was being installed on. The **`sqlite-devel-3.3.5-1`** and **`libsqlite-3.2.1-1`** packages must be removed before installing this component.	
224994	CEP currently logs any authentication failures during enrollment to the system log. These should log to the audit log.	
228932	The Cisco router may sometimes print an "abort" message when trying to download the CA certificate chain from a sub-ordinate. This is only a warning message and can be ignored.	

[10] https://bugzilla.redhat.com/show_bug.cgi?id=234887

Bug Number	Description	Workaround
229246	There is no separate SSL port for clients to authenticate to the RA.	See *Section 4.2, "Manually Adding a New Port to the RA"* for workaround isntructions.
230914	AEP is supported in Certificate System 7.3, although it is currently not documented.	
233024	The auto enrollment proxy configuration is not added to everyone's profile. This is typically occurs when configuring the AEP proxy on Windows child domains where the local administrator does not have permission to modify the **`cn=configuration`** tree in Active Directory. The simplest workaround is to use the **`Run as ..`** option to authenticate as the primary domain controller administrator and to then try to modify the **`cn=configuration`**. This relates to the **Populate AD** option in AEP.	
234884	The Phone Home UI pops up for both enrolled and un-initialized tokens on RHEL4 and MAC OS X, even though the tokens contain phoneHome URLs.	Type in the Phone Home URL and proceed.
234887	The Enterprise Security Client diagnostics logs are not visible in the diagnostics window.	See *Section 4.3, "Viewing Enterprise Security Client Diagnostics Logs"* for workaround isntructions.
235150	The TKS sub-system start/stop script currently does not check that the package is installed before attempting to execute.	
236795	In the Enterprise Security Client, the security officer mode does not work on MAC OS X.	
236857	In the RA agent page, the RA attempts to retrieve revocation information for a certificate that the agent does not have the rights to see. This is not an issue at present and can be ignored.	
236982	During certificate approval, the RA returns a message the the assigned serial number is unavailable. This problem only occurs on the approval page. If the user views the request again, the correct serial number will be shown. This will be fixed in the next release.	
237042	The TPS may refuse to enroll a new token if there are multiple token entries for the same user.	In the TPS agent page, delete one of the duplicate tokens.
237050	There can be numerous *File does not exist* errors in the RA error logs. The administrator can safely ignore these error messages.	
237056	On the agent interface of the RA, the List Requests page displays the total number of certificate requests. On the List Certificates page, the corresponding information is missing. This will be fixed in the next release.	
237250	There is currently no facility for canceling certificate revocation. This will be added in the next release.	

Bug Number	Description	Workaround
237251	There is currently no option to add comments to a revocation request submitted through the RA. This is useful for agents if they are temporarily putting certificates on hold. This facility is currently only provided in the CA. It will be added to the RA in the next release.	
237305	The CA subsystem in Certificate System 7.3 does not process SCEP requests that have been previously submitted. This can result in an error message similar to the following: `1706.http-9080-Processor24 - [20/Apr/2007:05:47:23 PDT] [20] [3] CEP Enrollment: Enrollment failed: user used duplicate transaction ID.`	To avoid this situation, ensure that the Cisco router generates fresh sets of keys for SCEP enrollments.
237353	If the user clicks a link in the agent interface too fast and too many times, the server may return *Broken pipe: core_output_filter: writing data to the network* and terminate the SSL connection.	Re-authenticate to the agent interface.
238039	The Subject Alt Name extension in certificates that are issued using the caDirUserCert profile will contain variables in un-substituted fashion (for example, **`$request.requestor_email$`**), if the profile request does not contain values available for substitution.	
238203	The TPS instance name is hardcoded in the **`CS.cfg`**. Because the instance name is hard-coded, the TPS looks for the configuration file in **`/var/lib/rhpki-tps/conf/CS.cfg`**.	If you create an instance with a name other than **`rhpki-tps`**, modify the **`/var/lib/`***tps-instance-name*`**/cgi-bin/sow/cfg.pl`** file to remove the hard-coded instance name.
453051	There are exception errors when trying to install a renewed certificate in the subsystem certificate database through the administrative console.	Instead of using the Console to install renewed subsystem certificates, use the **`certutil`** utility.

Table 4. Other Known Issues for Red Hat Certificate System 7.3

5. Documentation

The Red Hat Certificate System 7.3 documentation includes the following manuals:

- *Certificate System Administrator's Guide* explains all administrative functions for the Certificate System, such as adding users, creating and renewing certificates, managing smart cards, publishing CRLs, and modifying subsystem settings like port numbers.
- *Certificate System Agent's Guide* details how to perform agent operations for the CA, DRM, OCSP, and TPS subsystems through the Certificate System agent services interfaces.
- *Certificate System Enterprise Security Client Guide* explains how to install, configure, and use the Enterprise Security Client, the user client application for managing smart cards, user certificates, and user keys.

6. Copyright and Third-Party Acknowledgments

Copyrights and third-party acknowledgments for portions of Red Hat Certificate System 7.3 servers include the following:

Apache Software Foundation

Red Hat Certificate System TPS subsystems require a locally-installed Apache 2.0.x HTTP server. Although a local copy of this server is generally installed as part of the operating system (with its corresponding license located in **/usr/share/doc/***httpd-version***/LICENSE**, the latest version of this server is available at the following URL:

http://httpd.apache.org

Red Hat Certificate System CA, DRM, OCSP, and TKS subsystems use a locally-installed Tomcat 5.5 web server. Although an appropriate server is installed when any of these subsystems are installed, the latest version of this server is available at the following URL:

http://tomcat.apache.org

Red Hat Certificate System uses many components made available from Apache.

- The XML project jars are **crimson.jar** and **xalan.jar**. These are available at the following URL:

  http://xml.apache.org [11]

- The Tomcat project jar files are **servlet.jar** and **jakarta-naming.jar**. These are available at the following URL:

  http://jakarta.apache.org/tomcat/index.html [12]

Mozilla Foundation

Red Hat Certificate System uses version 4.2 of the Java™ Security Services (JSS) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of and, potentially, the binary images for newer versions are available at the following URL:

http://www.mozilla.org/projects/security/pki/jss/index.html [13]

Red Hat Certificate System also uses version 4.6 of the Netscape Portable Runtime (NSPR) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, the binary images for newer versions are available at the following URL:

http://www.mozilla.org/projects/nspr/index.html [14]

Additionally, Red Hat Certificate System uses version 3.11 of the Network Security Services (NSS) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, the binary images for newer versions are available at the following URL:

http://www.mozilla.org/projects/security/pki/nss/index.html

[13] http://www.mozilla.org/projects/security/pki/jss/index.html
[14] http://www.mozilla.org/projects/nspr/index.html

Red Hat Certificate System includes a set of compiled binaries (from NSS 3.11) of several tools from the Mozilla Project provided for the convenience of the user. This includes **`certutil`**, **`cmsutil`**, **`modutil`**, **`pk12util`**, **`signtool`**, **`signver`**, and **`ssltap`**. If any problems are found in these specific tools, the source code and build instructions for the latest version of this tool and, potentially, a binary image for other newer tools are available at the following URL:

http://www.mozilla.org/projects/security/pki/nss/tools/index.html [15]

Red Hat Certificate System includes version 1.5 R3 of Rhino JavaScript for Java™. If any problems are found in this specific distribution, the source code and build instructions for the latest version and, potentially, a binary image are available at the following URL:

http://www.mozilla.org/rhino/index.html [16]

Red Hat

Red Hat Certificate System requires a complete Red Hat Directory Server 7.1 or 8.x binary.

The open source portion of Certificate System is available at *https://rhn.redhat.com* [17].

Copyrights and third-party acknowledgments for portions of Red Hat Certificate System 7.3 clients include the following:

Mozilla Foundation

USE AND AVAILABILITY OF OPEN SOURCE CODE. Portions of the Product were created using source code governed by the Mozilla Public License (MPL). The source code for the portions of the Product governed by the MPL is available from *http://www.mozilla.org* under those licenses.

Red Hat Enterprise Security Client uses the latest version of the XULRunner cross-platform package. XULRunner is a Mozilla runtime package that can be used to bootstrap XUL+XPCOM applications that are as rich as Firefox and Thunderbird. If any problems are found in this specific distribution, the source code and build instructions for the latest versions and, potentially, a binary image are available at the following URL:

http://developer.mozilla.org/en/docs/XULRunner_1.8.0.1_Release_Notes [18]

Red Hat Enterprise Security Client also uses the Netscape Portable Runtime (NSPR) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, binary images for newer versions are available at the following URL:

http://www.mozilla.org/projects/nspr/index.html [19]

Red Hat Enterprise Security Client also uses the Network Security Services (NSS) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, binary images for newer versions are available at the following URL:

http://www.mozilla.org/projects/security/pki/nss/index.html

Additional Red Hat Enterprise Security Client smart card libraries and modules:

[15] http://www.mozilla.org/projects/security/pki/nss/tools/index.html
[16] http://www.mozilla.org/rhino/index.html
[17] https://rhn.redhat.com
[18] http://developer.mozilla.org/en/docs/XULRunner_1.8.0.1_Release_Notes
[19] http://www.mozilla.org/projects/nspr/index.html

- e-gate Smart Card Drivers for Windows 2000/XP Copyright 2002-2003 Schlumberger. All rights reserved.
- e-gate Smart Card Driver for Mac OS X Copyright 2003 by Chaskiel Grundman.

  Copyright 2003 by Philip Edelbrock.

  Significantly based on the Alladin etoken driver (the T=1 code is not needed): Copyright 2002 by Andreas Jellinghaus.

  Copyright 2002 by Olaf Kirch.

  See license terms below for rights on both parts.

  Some header files are from the pcsclite distribution: Copyright 1999 David Corcoran.
- MUSCLE smart card middleware and applets

  Copyright 1999-2002 David Corcoran.

  Copyright 2002 Schlumberger Network Solution.

  All rights reserved.

The following license terms govern the identified modules and libraries:

- e-gate Smart Card Drivers for Windows 2000/XP:

  Limited Warranty/ Exclusive Remedies. Schlumberger warrants to the benefit of Customer only, for a term of sixty (60) days from the date of acquisition of the e-gate Smart Card ("Warranty Term"), that if operated as directed under normal use and service, the Software will substantially perform the functions described in its applicable documentation. Schlumberger does not warrant that the Software will meet Customer's requirements or will operate in combinations that Customer may select for use, or that the operation of the Software will be uninterrupted or error-free, or that all Software errors will be corrected. Schlumberger's sole obligation and liability under this limited warranty shall be, at Schlumberger's option, to remedy any substantial non-performance of the Software to the functional descriptions set forth in its applicable documentation. If Schlumberger is unable to satisfy the foregoing limited warranty obligations during the Warranty Term, then Schlumberger shall, upon Customer's written request for termination of this Agreement, refund to Customer all sums paid to Schlumberger for the licensing of the Software hereunder. These are Customer's sole and exclusive remedies for any breach of warranty.

  WARRANTY DISCLAIMER. EXCEPT FOR THE EXPRESS LIMITED WARRANTY SET FORTH IN SECTION 5 ABOVE, THE SOFTWARE IS PROVIDED AS IS. SCHLUMBERGER AND ITS SUPPLIERS MAKE NO OTHER EXPRESS WARRANTIES. TO THE EXTENT AUTHORIZED BY APPLICABLE LAW, ALL OTHER WARRANTIES WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT, ARE SPECIFICALLY DISCLAIMED. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS AGREEMENT.

  Limitation of Liability. Schlumberger's cumulative liability to Customer, or any third party, for loss or damages resulting from any claim, demand or action arising out of or relating to this Agreement or use of the Software ("Damages"), shall not exceed the net amount paid to Schlumberger for the licensing of the Software, in this case, the cost of the single e-gate Smart Card. In no event

shall Schlumberger or any Supplier be liable for any indirect, incidental, special consequential or exemplary damages of any character, including, without limitation, damages for lost profits, goodwill, work stoppage, computer failure and all other commercial damages.

- e-gate Smart Card Driver for Mac OS X:

  Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

  - Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
  - Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
  - The names of its contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

  THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

- MUSCLE smart card middleware and applets:

  Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

  1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
  2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
  3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

  THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE

OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

7. Document History

Revision 7.3.5 August 10, 2010 **Ella Deon Lackey** ***dlackey@redhat.com***

Adding warning note on Red Hat Directory Server requirements of conflict with mod_nss packages introduced with Errata RHSA-2010:0602.

Revision 7.3.4 April 10, 2010 **Ella Deon Lackey** ***dlackey@redhat.com***

Revising JRE/JDK section to recommend version from the latest errata updates.

Revision 7.3.3 March 25, 2010 **Ella Deon Lackey** ***dlackey@redhat.com***

Adding information on applying Errata 2010:0170 and reconfiguring subsystems.

Revision 7.3.2 Tue Jul 23 2007 **David O'Brien** ***david.obrien@redhat.com***

Revised list of supported platforms.

Revision 7.3.1 Mon Jun 4 2007 **David O'Brien** ***david.obrien@redhat.com***

Bugzilla 240259: Added link to documentation for Auto Enrollment Proxy on fedora project page.

Revision 7.3.0 Tue May 1 2007 **David O'Brien** ***david.obrien@redhat.com***

Added revision history.